1924

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/716,221	11/21/2000	Hisashi Inoue	2000 1451A	9406

7590 11/23/2004

Wenderoth Lind & Ponack LLP
2033 K Street NW
Suite 800
Washington, DC 20006

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/716,221	INOUE ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to request for reconsideration filed on August 09, 2004. Original application contained Claims 1 – 18. Applicant has amended Claims 1 – 18. No Claims were canceled. Therefore, presently pending claims are 1 – 18.

Response to Arguments

2. Applicant's arguments filed on August 09, 2004, have been fully considered but they are not persuasive for the following reasons:

Regarding independent amended claims 1, 7 and 13, applicant argued that the cited prior arts (CPA) [Nakamura et al. U.S. Patent Number 6,185,312 and Barton U.S. Patent Number 6,047,374] even when taken together, do not teach, "generate authentication data from the pseudo-random number series " and "embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA". These arguments are not found persuasive. CPA clearly teaches and applicant agrees (see page 18 of Remarks) an apparatus for embedding information comprising a blocking step for dividing data to be processed into blocks; an information embedding step for embedding watermark-information. CPA discloses "data generating a pseudo-random number series by using predetermined key data and generating data from the pseudo-random number series" (Nakamura Column 5 lines 42 – 55) and "authentication

data generation" (Barton Column 4 lines 22 – 42 and Column 7 line 5 – Column 8 line 28). CPA also discloses, "embedding the authentication data in transform coefficients of a lowest frequency bands exclusive of the MRA" (Nakamura Column 6 lines 4 – 57 and Column 12 lines 14 – 50). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, into transforming coefficients of frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding generated authenticated information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding independent amended claims 3, 9 and 15, applicant argued that the cited prior arts (CPA) [Nakamura et al. U.S. Patent Number 6,185,312 and Barton U.S. Patent Number 6,047,374] even when taken together, do not teach, "generate authentication data from the pseudo-random number series " and "extracting embedded information embedded based on the key data by the specific apparatus from transform coefficients of a lowest frequency bands exclusive of the MRA". These arguments are not found persuasive. CPA clearly teaches and applicant agrees (see page 18 of Remarks) an apparatus for embedding information comprising a blocking step for dividing data to be processed into blocks; an information embedding step for embedding watermark-information. CPA discloses "data generating a pseudo-random number

series by using predetermined key data and generating data from the pseudo-random number series" (Nakamura Column 5 lines 42 – 55) and "authentication data generation" (Barton Column 4 lines 22 – 42 and Column 7 line 5 – Column 8 line 28). CPA also discloses, "extracting embedded information embedded based on the key data by the specific apparatus from transform coefficients of a lowest frequency bands exclusive of the MRA" (Nakamura Column 6 lines 4 – 57; Column 12 lines 14 – 50 and Barton Column 4 lines 22 – 41 and Column 7 line 5 – Column 8 line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information and then extract the embedded authentication information as taught by Barton, into transforming coefficients of frequency bands as taught by Nakamura to provide a method of embedding and extracting digital image by embedding generated authenticated information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Applicant has argued that Page 4 of the office action indicates that CPA-Nakamura "does not explicitly teach generating authentication data from the pseudo-random number series" and CPA-Barton fails to teach "authentication data is generated from a pseudo-random series". Examiner redirects applicant to Page 4 of the office action to further explain that CPA-Nakamura does not explicitly teach generating "authentication" data from the pseudo-random series and does explicitly teach

generating data from the pseudo-random number series and CPA-Barton explicitly teach generating and embedding "authentication" information. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information and then extract the embedded authentication information as taught by Barton, into transforming coefficients of frequency bands as taught by Nakamura to provide a method of embedding and extracting digital image by embedding generated authenticated information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Applicant has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that CPA does teach or suggest the subject matter broadly recited in independent claims 1, 3, 7, 9, 13 and 15. Dependent claims 2, 4 – 6, 8, 10 – 12, 14 and 16 - 18 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 1 – 18 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1- 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura et al. (U.S. Patent No. 6,185,312) in view of Barton (U.S. Patent No. 6,047,374 hereinafter "Barton").

Regarding Claim 1, Nakamura teaches and describes a tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal, (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), the apparatus comprising:

a band division portion operable to divide the digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 44);

an authentication data generation portion operable to generate a pseudo-random number series by using predetermined key data, and generate authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

a key data embedding portion operable to embed the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 #22, 23 and Column 6 lines 4 – 57);

an authentication data embedding portion operable to embed the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46); and

a band synthesis portion operable to reconstruct the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16, Column 15 line 25 – Column 18 line 57 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing

tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 3, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), the tamper detecting apparatus comprising:

a band division portion operable to divide the digital image signal into a plurality of frequency bands (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43);

a key data extraction portion operable to extract key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 # 22, 23 and Column 6 lines 4 – 57). Nakamura does not explicitly disclose key data extraction means for extracting the key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands. However Barton discloses a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28),

an authentication data generation portion operable to generate a pseudo-random number series by using predetermined key data, and to generate authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

an embedded information extraction portion operable to extract embedded information embedded based on the key data by the specific apparatus from transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Barton Fig. 2 # 42, Column 4 lines 22 – 41 and Column 7 line 55 – Column 8 line 28); and

a tamper determination portion operable to compare the embedded information with the authentication data for verification and to determine whether the digital image has been tampered with (Barton Fig. 2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate, embed and extract the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding and extracting digital image with authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 7, Nakamura teaches and describes a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), said method comprising:

dividing the digital image signal into a plurality of frequency bands (Fig. 2 # 11 and Column 5 lines 42 – 44);

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 #31 and Column 5 lines 42 – 55);

embedding the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 and Column 6 lines 4 – 57);

embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46);

reconstructing the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of

embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 9, Nakamura teaches and describes a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), comprising:

dividing the digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 44);

extracting key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 # 22, 23 and Column 6 lines 4 – 57). Nakamura does not explicitly disclose extracting key data extraction means for extracting the key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands. However Barton discloses a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28),

generating a pseudo-random number series by using the key data, and generating authentication data from the pseudo-random number series (Fig. 3 #31 and Column 5 lines 42 – 55);

extracting embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46);

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28);

comparing the embedded formation with the authentication data for verification and determining whether the digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 13, Nakamura teaches and describes a recording medium on which a program having computer device readable instructions to be run on a computer device is recorded for carrying out a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), computer device readable instruction including instructions capable of instructing a computer device to perform the method comprising:

dividing the digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 44);

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

embedding the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46);

embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 and Column 17 line 46); and

reconstructing the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16, Column 15 line 25 – Column 18 line 57 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 15, Nakamura teaches and describes a recording medium on which a program having computer device readable instructions to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), computer device readable instructions including instructions capable of instructing a computer device to perform the method comprising:

dividing the digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 55);

extracting key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands;

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 # 22, 23 and Column 6 lines 4 – 57). Nakamura does not explicitly disclose key data extraction means for extracting the key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands. However Barton discloses a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28), and

comparing the embedded information with the authentication data for verification and determining whether the digital image has been tampered with (Barton Fig. 2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would

have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Nakamura teaches and describes a tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43),

wherein a set value T and a set value m are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38);

wherein said authentication data embedding portion embeds the authentication data in each transform coefficient of the MRR by comparing an absolute value of the transform coefficient with the set value T, and if the absolute value is less than the set value T, setting the transform coefficient to the set value +m or –m depending on the bit value of the authentication data to be embedded, and if the absolute value is not less than the set value T, setting the transform coefficient to an even or odd integer nearest

to the value q depending on the bit value of the authentication data to be embedded, and where T is a positive integer and m is an integer not more that T (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein said tamper determination portion comprises:

a block division portion operable to divide the digital image into a plurality of unit blocks each composed on a predetermined number of pixels (Fig. 2 # 11, Column 5 lines 42 – 44; Fig. 9, Column 14 line 61 – Column 15 line 55, Fig. 12, 13, Column 17 lines 21 – 32 and Fig. 25, 26, Column 23 lines 15 – 46);

a regional embedded information read portion operable to read, for each of the unit blocks, embedded information embedded in the transform coefficients of the MRR that represents the same spatial region as the unit block, serially from all of the embedded information extracted by the embedded information extraction portion (Fig. 10, Column 16 lines 17 – 37);

a regional authentication data read portion operable to read, for each of the unit blocks, authentication data corresponding in position to the embedded information serially read by the regional embedded information read means, serially from all of the

authentication data generated by the authentication data generation portion (Fig. 10, Column 16 lines 17 – 53 and Fig. 35 Column 28 line 5 – Column 29 line 41); and

a block-tamper determination portion operable to compare the embedded information serially read with the authentication data serially read and determining, for each of the unit blocks, whether the digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 5 is rejected as applied above in rejecting claim 3. Furthermore, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43),

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38),

wherein said embedded information extraction portion extracts the embedded information from each transform coefficient of the MRR by comparing an absolute value of the transform coefficient with the set value T, and if the absolute value is less than the set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information in the transform coefficient based on the determination, and if the absolute value is not less than the set value T, determining whether the value q is even or odd and extracting a bit value of embedded

information embedded in the transform coefficient based on the determination, and wherein T is a positive integer (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Nakamura teaches and describes a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43),

wherein a set value T and a set value m are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38); and

wherein embedding authentication data includes comparing an absolute value of the transform coefficient with the set value T, and if the absolute value is less than the set value T;

setting the transform coefficient to the set value +m or –m depending on the bit value of the authentication data to be embedded, and if the absolute value is not less than the set value T; and

setting the transform coefficient to an even or odd integer nearest to the value q depending on the bit value of the authentication data to be embedded if the absolute value is not less than the set value T, and wherein T is positive integer and m is an

integer not more than T (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Nakamura teaches and describes a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), further comprising

dividing the digital image into a plurality of unit blocks each composed on a predetermined number of pixels (Fig. 2 # 11, Column 5 lines 42 – 44; Fig. 9, Column 14 line 61 – Column 15 line 55, Fig. 12, 13, Column 17 lines 21 – 32 and Fig. 25, 26, Column 23 lines 15 – 46);

reading, for each of the unit blocks, embedded information embedded in the transform coefficients of the MRR that represents the same spatial region as the unit block, serially from all of the embedded information (Fig. 10, Column 16 lines 17 – 37);

reading, for each of the unit blocks, authentication data corresponding in position to the embedded information serially read, serially from all of the authentication data (Fig. 10, Column 16 lines 17 – 53 and Fig. 35 Column 28 line 5 – Column 29 line 41); and

comparing a series of the embedded formation serially read with a series of the authentication data serially read and determining, for each of the unit blocks, whether

the digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 11 is rejected as applied above in rejecting claim 9. Furthermore, Nakamura teaches and describes a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43),

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38),

wherein said extracting embedded information includes comparing an absolute value of the transform coefficient with the set value T;

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than the set value T, and extracting a bit value of embedded information in the transform coefficient based on the determination;

determining whether the value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and wherein T is a positive integer (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43),

wherein a set value and a set value m are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38);

wherein said embedding authentication data includes:

comparing an absolute value of the transform coefficient with the set value T, and if the absolute value is less than the set value T,

setting the transform coefficient to the set value +m or –m depending on the bit value of the authentication data to be embedded, and if the absolute value is not less than the set value T, and

setting the transform coefficient to an even or odd integer nearest to the value q depending on the bit value of the authentication data to be embedded if the absolute value is not less than the set value T, and wherein T is a positive integer and m is an integer not more than T (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein the computer device to perform the method further comprising:

dividing the digital image into a plurality of unit blocks each composed on a predetermined number of pixels (Fig. 2 # 11, Column 5 lines 42 – 44; Fig. 9, Column 14 line 61 – Column 15 line 55, Fig. 12, 13, Column 17 lines 21 – 32 and Fig. 25, 26, Column 23 lines 15 – 46);

reading, for each of the unit blocks, embedded information embedded in the transform coefficients of the MRR that represents the same spatial region as the unit block, serially from all of the embedded information (Fig. 10, Column 16 lines 17 – 37);

reading, for each of the unit blocks, authentication data corresponding in position to the embedded information serially read, serially from all of the authentication data (Fig. 10, Column 16 lines 17 – 53 and Fig. 35 Column 28 line 5 – Column 29 line 41); and

comparing a series of the embedded formation serially read with a series of the authentication data serially read and determining, for each of the unit blocks, whether the digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 17 is rejected as applied above in rejecting claim 15. Furthermore, Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43),

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38),

wherein said extracting embedded information includes comparing an absolute value of the transform coefficient with the set value T;

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than the set value T, and extracting a bit value of embedded information in the transform coefficient based on the determination, and

determining whether the value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and wherein T is a positive integer (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 6 is rejected as applied above in rejecting claim 4. Furthermore, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43),

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38),

wherein said embedded information extraction portion extracts the embedded information from each transform coefficient of the MRR by comparing an absolute value of the transform coefficient with the set value T, and if the absolute value is less than the set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information in the transform coefficient based on the determination, and if the absolute value is not less than the set value T, determining whether the value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and wherein T is a positive integer (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 12 is rejected as applied above in rejecting claim 10. Furthermore, Nakamura teaches and describes a tamper detecting method of detecting tamper with a

digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43),

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38),

wherein said extracting embedded information includes comparing an absolute value of the transform coefficient with the set value T,

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than the set value T, and extracting a bit value of embedded information in the transform coefficient based on the determination, and

determining whether the value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and wherein T is a positive integer (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 18 is rejected as applied above in rejecting claim 16. Furthermore, Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a

specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43),

wherein a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38),

wherein said extracting embedded information includes comparing an absolute value of the transform coefficient with the set value T,

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than the set value T, and extracting a bit value of embedded information in the transform coefficient based on the determination, and

determining whether the value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and wherein T is a positive integer (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
November 15, 2004.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100